Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Sanja Novaković

Digitalni potpis

Završni rad

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Sanja Novaković

Digitalni potpis

Završni rad

Voditelj: izv.prof.dr.sc. Ivan Matić

Osijek, 2016.

Sažetak. U ovom radu proučavamo digitalni potpis te neke od tehnika koje služe za njegovu izradu u teoriji i praksi. Najprije se dotićemo RSA algoritma koji su prvi puta javno opisali Ron Rivest, Adi Shamir i Leonard Adleman 1977. godine. To je prvi algoritam prikladan za potpisivanje i enkripciju podataka te se, pod pretpostavkom korištenja dovoljno dugih ključeva i ažurnih implementacija, smatra sigurnim. Nakon toga ćemo obraditi i Rabinovu shemu potpisa, zasnovanu na težini određivanja kvadratnih korijena modulo fiksni složeni broj. Pokazuje se da je ovaj važan problem ekvivalentan problemu faktorizacije prirodnih brojeva.

Ključne riječi: digitalni potpis, RSA kriptosustav, šifriranje, dešifriranje, Rabinov kriptosustav

Abstract. In this paper we study the digital signature, and some of the techniques serve for the development of the theory and practice. First touches on RSA algorithm for the first time publicly described by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. It is the first algorithm suitable for signing and data encryption, assuming the use of sufficiently long keys and timely implementation, considered safe. We will then process and the Rabin signature scheme, based on the weight determination square root modulo a fixed complex number. It turns out that this important problem equivalent to the problem of factorization of natural numbers n.

Key words: digital signature, RSA cryptosystem, encryption, decryption, Rabin cryptosystem

Sadržaj

1 Uvod

Digitalni potpisi predstavljaju podskupinu elektroničkih potpisa koji koriste različite kriptografske metode. Zbog toga je razvoj digitalnog potpisa usko vezan uz povijest kriptografije. Digitalni potpis poruke je broj ovisan o tajni koja je poznata samo potpisniku i dodatno sadržaju poruke koja je potpisana. Potpis mora biti provjerljiv, u slučaju ako se pojavi spor o tome da li je stranka potpisala dokument. Digitalni potpisi imaju mnoge primjene u području informacijske sigurnosti, uključujući autentifikaciju i integritet podataka. Jedna od najznačajnijih primjena digitalnog potpisa je ovjera javnih ključeva u velikim mrežama. Pojam i korisnost digitalnog potpisa su prepoznati nekoliko godina prije nego što je praktična realizacija bila dostupna. Prva metoda koja je otkrivena bio je RSA sustav za potpisivanje, koja ostaje i danas jedna od najvažnijih praktičnih i najsvestranijih raspoloživih tehnika.

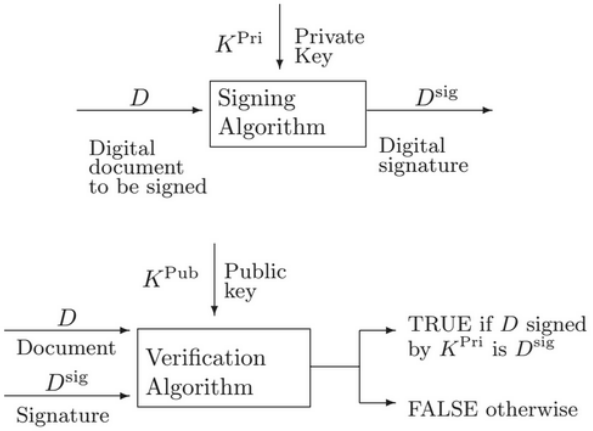
2 Što je digitalni potpis?

Shema šifriranja, bila simetrična ili asimetrična, rješava problem sigurne komunikacije preko nesigurne mreže. Digitalni potpisi rješavaju drugačiji problem, analogan potpisu tintom ili olovkom na dokument. Zanimljivo je da su alati koji se koriste za izgradnju digitalnog potpisa vrlo slični alatima koji se koriste za izgradnju asimetrične šifre.

Pokažimo problem koji bi digitalni potpis trebao riješiti. Samantha ima (digitalni) dokument D, primjerice računalnu datoteku, a ona želi stvoriti neki dodatan dio informacija D^{Sam} koje se može koristiti kao uvjerljiv dokaz da Samantha odobrava dokument. Tako možete vidjeti Samanthin digitalni potpis D^{Sam} kao analogon njezinom stvarnom potpisu kojeg koristi na običnom dokumentu.

Kao usporedba svrhe i funkcionalnosti javnog ključa (asimetričnih) kriptiranih sustava nasuprot digitalnog potpisa, smatramo analogiju bankovnog depozitnog trezora i pečatnog prstena. Bankovno depozitni trezor ima uski ulaz ("javni ključ za šifriranje") u koju svatko može položiti omotnicu, ali samo vlasnik kombinacije ("privatnog ključa za dešifriranje") može otvoriti bravu trezora i pročitati poruku. Tako je javnim ključem kriptosustav digitalna verzija bankovnog depozitnog trezora. Pečatnjak ("privatno potpisivanje kao ključ") je prsten koji ima udubljenu sliku. Vlasnik kaplje vosak iz svijeće na njegov dokument i pritišće prsten u vosak kako bi ostavio otisak ("javni potpis"). Svatko tko gleda na dokumentu može provjeriti je li utisak u vosku napravljen od strane vlasnika prstena, ali samo je vlasnik prstena u stanju stvoriti valjane otiske. Tako se može prikazati sustav digitalnog potpisa kao moderna verzija pečatnog prstena.

Unatoč njihovim različitim namjenama, sheme digitalnog potpisa su slične asimetričnim kriptosustavima u tome što uključuju javne i privatne ključeve te uključuju algoritme koji koriste te ključeve.



Slika 1: Sheme dviju komponenti digitalnog potpisa

Opis dijelova koji čine shemu digitalnog potpisa:

- K^{Pri} Privatni potpis
- K^{pub} Javni ključ
- *Potpis* Algoritam za potpisivanje koji kao ulaz uzima digitalni dokument D i privatni ključ K^{Pri} i vraća potpis D^{sig} za D.
- *Provjera* Algoritam za provjeru koji kao ulaz uzima digitalni dokument D, potpis D^{sig} i javni ključ K^{pub}. Algoritam vraća potvrdu ako je D^{sig} potpis za D koji odgovara privatnom ključu K^{Pri}, u suprotnom vraća pogrešku.

Operacija digitalnog potpisa je prikazana na Slici 1. Važno je primjetiti kako na Slici 1 algoritam provjere ne zna privatni ključ K^{Pri} kad utvđuje da li je D potpisan sa K^{Pri} jednak D^{sig}. Algoritam za provjeru ima pristup samo javnom ključu K^{Pub}. Nije teško konstruirati (beskorisne) algoritme koji zadovoljavaju svojstva digitalnog potpisa. Na primjer, neka je $K^{pub} = K^{Pri}$. No, teško je stvoriti shemu digitalnog potpisa u kojoj je vlasnik privatnog ključa K^{Pri} u stanju stvoriti valjane potpise, ali iz javnog ključa K^{Pub} ne možemo otkriti privatni ključ K^{Pri}. Za siguran digitalni potpis su potrebni idući uvjeti:

- Dan je K^{Pub}, provalnik ne može otkriti K^{Pri} , niti on može odrediti bilo koji drugi privatni ključ koji proizvodi iste potpise kao K^{Pri}.
- Dan je K^{Pub} i popis potpisanih dokumenata $D_1, \ldots, D_n$ sa njihovim potpisima $D_1^{sig}, \ldots, D_n^{sig}$, provalnik ne može točno odrediti valjani potpis za bilo koji dokument D koji nije na popisu $D_1, \ldots, D_n$.

Drugi uvjet je prilično drugačiji od situacije za shemu šifriranja. U šifriranju javnog ključa, provalnik može stvoriti onoliko šifriranih/otvorenih tekstova koliko želi, jer on ih može stvoriti pomoću poznatog javnog ključa. Međutim, digitalni potpis svaki put za potpisivanje koristi novi dokument, on otkriva novi dokument / par potpisa, koji pruža nove informacije provalniku. Drugi uvjet kaže da provalnik ne dobiva ništa osim poznavanja tog novog para. Napad na digitalni potpis koja omogućuje korištenje velikog broja poznatih potpisa naziva se napad prijepisa.

Napomena 2.1. *Digitalni potpisi su jednako važni kao javni ključ kriptosustava za poslovanje u digitalnom dobu, i mogli bi postati od sve veće važnosti. Kao značajni primjer, vaše računalo nesumnjivo prima programe i nadogradnje sustava preko Interneta. Kako bi vaše računalo moglo potvrditi da nadogradnja dolazi iz sigurnih izvora, kroz nešto bi trebao dobiti naziv tvrtke koja nam pruža nadogradnju? A to je digitalni potpis. Izvorni program dolazi opremljen s javnim ključem za provjeru od tvrtke. Tvrtka koristi privatni potpis kao ključ za potpisivanje nadogradnje i šalje vašem računalu novi program i potpis. Vaše računalo može koristiti javni ključ za provjeru potpisa, čime potvrđuje da program dolazi iz pouzdanog izvora, prije nego što ga instalirate na vašem sustavu.*

Moramo naglasiti da iako je to ideja kako se digitalni potpis može koristiti, ovo je znatno pojednostavljeno objašnjenje. U stvarnom svijetu primjene digitalnih potpisa programa zahtijevaju znatnu vještinu za izbjegavanje velikih sigurnosnih problema.

Napomena 2.2. *Prirodna sposobnost većine digitalnih potpisa je potpisati samo malu količinu podataka, recimo broj bitova b, gdje je b između* 80 *i* 1000. *To je dakle, prilično neučinkovito za potpisati veliki digitalni dokument D, zato što oduzima puno vremena da provjerite svaki b bitova dokumenta D jer će rezultat dobivenog digitalnog potpisa vjerojatno biti velik kao i u izvornom dokumentu.*

Rješenje ovakvog problema je korištenje takozvane hash funkcije, koja je lakša za izračunavanje,

$$\text{Hash} : (\text{proizvoljna veličina dokumenta}) \to \{0,1\}^k$$

a vrlo ju je teško invertirati. Općenito, želimo da bude vrlo teško pronaći dva različita inputa D i D' čiji su outputi $Hash\ (D)$ i $Hash\ (D')$ isti. Zatim, umjesto da potpisuje svoj dokument D, Samantha izračunava i potpisuje $Hash\ (D)$. Za provjeru, Victor izračunava i provjerava potpis za $Hash\ (D)$.

3 RSA digitalni potpis

U ovom radu ćemo opisati obje poznate RSA sheme- RSA enkripcija i RSA digitalni potpis. Ideja je vrlo jednostavna. Za RSA digitalni potpis ideja je ista kao i za RSA enkripciju, Samantha se odluči za dva dovoljno velika prosta broja p i q koji su poznati samo njoj, a zatim objavljuje svoj produkt $N = pq$ i javnu provjeru eksponenta v. Samantha koristi svoje znanje o faktorizaciji broja N za rješavanje kongruencije

$$sv \equiv 1 \pmod{(p-1)(q-1)}. \tag{3.1}$$

Imajmo na umu da ako je Samantha radila RSA enkripciju, onda v treba biti njen enkripcijski eksponent i s treba biti njezin eksponent za dešifriranje. Međutim sad je s njezin eksponent za potpisivanje, a v eksponent za provjeru. Da biste se prijavili u digitalni dokument D koji pretpostavljamo da je cijeli broj u rasponu od 1 do N, Samantha izračunava

$$S \equiv D^s \pmod{N}.$$

Viktor provjerava valjanost potpisa S na D izračunavajući

$$S^v \pmod{N},$$

te provjerava da li je to jednako D.

Teorem 3.1 (Eulerova formula za $p \cdot q$)**.** *Neka su p i q različiti prosti brojevi i neka je*

$$g = (p-1, q-1).$$

Tada je

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq}, \textit{ za svaki } a \textit{ koji zadovoljava } (a, pq) = 1.$$

Općenito, ako su p i q neparni prosti brojevi tada je

$$a^{(p-1)(q-1)/2} \equiv 1 \pmod{pq}, \textit{ za svaki } a \textit{ koji zadovoljava } (a, pq) = 1.$$

Ovaj postupak je ispravan jer nam Eulerova formula za pq govori da je

$$S^v \equiv D^{sv} \equiv D \pmod{N}.$$

Shema RSA digitalnog potpisa sažeta je u Tablici 1.

Samantha	Victor
Kreiranje ključa	
Izabere tajne proste brojeve p i q. Izabere eksponent v za provjeru takav da je $(v,(p-1)(q-1))=1$. Objavljuje $N=pq$ i v.	
Potpisivanje	
Izračunava s koji zadovoljava $sv \equiv 1 \pmod{(p-1)(q-1)}$. Potpisuje dokument D računajući $S \equiv D^s \pmod{N}$.	
Provjera	
	Izračunava $S^v \pmod{N}$ i potvrđuje da je to jednako D.

Tablica 1: RSA digitalni potpis

Ako Eva ima faktor N, može rješiti formulu (3.1) s kojom je zadano potpisivanje Samanthinim tajnim ključem s. Međutim, kao i sa RSA enkripcijom, veliki problem RSA digitalnog potpisa nije izravno problem faktorizacije. Da bi krivotvorila potpis na dokument D, Eva treba pronaći v-ti korijen od D modulo N. To je upravo analogon dešifriranju teškog RSA problema, u kojem je otvoreni tekst e-ti korijen šifriranog teksta.

Napomena 3.2. *Kao i kod RSA enkripcije, možemo dobiti na učinkovitosti odabirom s i v koji zadovoljavaju*

$$sv \equiv 1 \pmod{\frac{(p-1)(q-1)}{gcd(p-1,q-1)}}.$$

Eulerova formula za pq osigurava da postupak i dalje radi.

Primjer 3.3. *Prikazujemo shemu digitalnog potpisa malim numeričkim primjerom.*
RSA stvaranje ključa za potpisivanje

- *Samantha izabire dva tajna prosta broja $p = 1223$ i $q = 1987$ i izračunava njen javni modul:*
  $N = p \cdot q = 1223 \cdot 1987 = 2430101$.
- *Samantha izabire javni eksponent provjere $v = 948047$ sa svojstvom*
  $gcd(v,(p-1)(q-1)) = gcd(948047, 2426892) = 1$.

RSA prijava

- *Samantha računa njen privatni ključ za potpisivanje koristeći tajni broj p i q te izračunava $(p-1)(q-1) = 1222 \cdot 1986 = 2426892$ i onda rješava kongruenciju*
  $vs \equiv 1 \pmod{(p-1)(q-1)}$, $948047 \cdot s \equiv 1 \pmod{2426892}$.
- *Samantha odabire digitalni dokument za prijavu $D = 1070777$ takav da je $1 \leq D < N$.*
- *Izračunava digitalni potpis*
  $S \equiv D^s \pmod{N}$, $S \equiv 1070777948047 \equiv 1473513 \pmod{2430101}$.
- *Samantha objavljuje dokument i potpis: $D = 1070777$ i $S = 1473513$.*

RSA provjera

- *Viktor koristi Samanthin javni modul N i eksponent v za provjeru da izračuna* $S^v \pmod{N}$, $14735131051235 \equiv 1070777 \pmod{2430101}$.
- *On provjerava da li je vrijednost od S^v modulo N jednaka kao vrijednost digitalnog dokumenta* $D = 1070777$.

4 Rabinova shema

Rabinova shema potpisa javnog ključa slična je RSA shemi, ali ona koristi javni eksponent e. Radi jednostavnosti, pretpostavlja se da je $e = 2$. Prostor potpisa M_s je $\mathbb{Q}_n$ (skup kvadratnih ostataka modulo n), a potpisi su njegovi kvadratni korijeni. Funkcija redundancije R izabire iz prostora poruke M u M_S, i to je javno poznata funkcija.

Definicija 4.1. *Neka je* $(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je* a *kvadratni ostatak modulo* m. *U protivnom kažemo da je* a *kvadratni neostatak modulo* m.

Primjer 4.2. $m = 5$

$$1^2 \equiv 1 \pmod{5}$$
$$2^2 \equiv 4 \pmod{5}$$
$$3^2 \equiv 4 \pmod{5}$$
$$4^2 \equiv 1 \pmod{5}$$

$1, 4$ *su kvadratni ostatci modulo* 5.

Algoritam 1: Pronalaženje kvadratnog korijena prostog broja $p \pmod{a}$.

Ulaz: Neparan prost broj p i a kvadratni ostatak modulo p.
Izlaz Dva kvadratna korijena od a modulo p.
1. Nasumično izabiremo $b \in \mathbb{Z}_p$ sve dok je $b^2 - 4 \cdot a$
kvadratni neostatak modulo p, $(\frac{b^2-4\cdot a}{p}) = -1$.
2. Neka je f polinom $x^2 - b \cdot x + a$ iz $Z_p[x]$
3. Izračunamo $r \equiv x^{(p+1)/2} \pmod{f}$
4. Vrati $(r, -r)$.

Algoritam 2: Pronalaženje kvadratnog korijena modulo n
gdje je n produkt danih prostih brojeva p i q.

Ulaz: Broj n, njegovi prosti faktori p i q, $a \in \mathbb{Q}_n$.
Izlaz: Četiri kvadratna korijena od a modulo n.
1. Koristimo prethodni algoritam za nalaženje dva kvadratna korijena
r i $-r$ od a modulo p.
2. Koristimo prethodni algoritam za nalaženje dva kvadratna korijena
s i $-s$ od a modulo q.
3. Koristeći prošireni Euklidov algoritam nalazimo brojeve c i d
takvi da je $c \cdot p + d \cdot q = 1$.
4. Postavimo $x \leftarrow (r \cdot d \cdot q + s \cdot c \cdot p) \pmod{n}$ i $y \leftarrow (r \cdot d \cdot q - s \cdot c \cdot p) \pmod{n}$.
Vrati $(\pm x \pmod{n}, \pm y \pmod{n})$.

Algoritam 3: Generiranje ključa za shemu javnog potpisivanja.

Svatko može stvoriti javni ključ i odgovarajući privatni ključ.
Svaka osoba A treba napraviti sljedeće:
1. Generirati dva velika različita prosta broja p i q, otprilike iste veličine.
2. Izračunati $n = p \cdot q$.
3. Javni ključ osobe A je n, a privatni ključ je (p, q).

Primjer 4.3. *Uzmimo dva različita prosta broja:* $p = 13$, $q = 15$.
Izračunamo $p \cdot q = 13 \cdot 15 = 195$ *Javni ključ je* 195, *a privatni* $(13, 15)$.

Algoritam 4: Generiranje Rabinovog potpisa i provjera

Osoba A šalje poruku $m \in M$. Svaka osoba B može provjeriti potpis osobe A i rekonstruirati poruku m iz potpisa.
1. Generiranje potpisa. Osoba A treba napraviti sljedeće:
   a) Izračunati $\acute{m} = R(m)$
   b) Izračunaj kvadratni korijen s iz $\acute{m} \pmod n$ (uz pomoć prethodnog algoritma).
   c) Potpis osobe A za poruku m je s.

Algoritam 5: Pronalaženje kvadratnog korijena modulo a prostog broja p, gdje je $p \equiv 3 \pmod 4$.

Ulaz: Neparan prost broj p gdje je je $p \equiv 3 \pmod 4$, $a \in \mathbb{Q}_p$.
Izlaz: Dva kvadratna korijena od a modulo p.
1. Izračunati $r \equiv a^{(p+1)/4} \pmod p$.
2. Vrati $(r, -r)$.

Primjer 4.4. *Generiranje Rabinovog potpisa sa izmišljenim malim parametrima.*
Generiranje ključa: Osoba A izabire proste brojeve $p = 11$, $q = 19$, *izračunamo* $n = 209$. *Javni ključ osobe A je* 209, *privatni* $(11, 19)$. *Prostor potpisa je* $M_s = \mathbb{Q}_{209} = \{1, 4, 5, 9, 16, 20, 23, 25, 26, 36, 42, 45, 47, 49, 58, 64, 80, 81, 82, 92, 93, 100, 102, 104, 111, 115, 119, 125, 130, 137, 144, 157, 158, 159, 163, 168, 169, 177, 180, 188, 191, 196, 199, 201, 207\}$.
Uzmimo $M = M_s$ *i neka je funkcija redundancije R identiteta* $\acute{m} = R(m) = m$.
Generiranje potpisa: Pošaljimo poruku $m = 23$, *A izračuna* $R(m) = \acute{m} = 23$, *i tada nađemo korijen od* $\acute{m}$ *modulo* 209. *Kako su 11 i 19 oba kongruentni 3 modulo 4 koristimo prethodni algoritam:*

$$m^2 \pmod n = 111$$
$$m^2 \equiv 111 \pmod{209}$$
$$m^2 \equiv 111 \pmod{11}$$
$$m^2 \equiv 111 \pmod{19}$$
$$111^{(11+1)/4} \equiv 1^3 \equiv 1 \pmod 1$$
$$111^{(19+1)/4} \equiv 16^5 \equiv 4 \pmod{19}$$
$$s \equiv \pm 1 \pmod{11}$$
$$s \equiv \pm 2 \pmod{19}$$

$s = 21, 78, 131, 188$.
Izabrali smo potpis za m, $s = 131$. *Potpis može biti bilo koji od navedena četiri kvadratna korijena.*
Provjera potpisa: Osoba B *izačunava* $\acute{m} \equiv s^2 \pmod{209} = 23$. $\acute{m} = 23 \in M_s$, B *prihvaća potpis i vraća* $m = R^{-1}(\acute{m}) = 23$.

Funkcija redundancije je ključna za sigurnost Rabinove sheme potpisa. Primjerice pretpostavimo da je $M = M_s = \mathbb{Q}_n$ i $R(m) = m$ za svaki $m \in M$. Ako napadač odabere bilo koji broj $s \in \mathbb{Z}_n$ i kvadrira ga $\acute{m} = s^2 \pmod{n}$, tada je s valjani potpis za $\acute{m}$, a dobiven je bez znanja privatnog ključa. U tom slučaju falsifikat je trivijalan.

Jedan nedostatak Rabinovog kriptosustava je da korištena funkcija $s^2 \pmod{n}$ nije injekcija. Postoje četiri kvadratna korijena modulo n pa dešifriranje nije moguće provesti na jedinstven način.
Williams je 1980. dao jednu modifikaciju Rabinovog kriptosustava kojom se također eliminira ovaj nedostatak. U toj modifikaciji se kreće od prostih brojeva p, q sa svojstvom $p \equiv 3 \pmod{8}$, $q \equiv 7 \pmod{8}$. Tada je Jacobijev simbol $(\frac{2}{pq}) = -1$, pa se svojstva Jacobijevog simbola mogu iskoristiti za identifikaciju "pravog" kvadratnog korijena.

Literatura

[1] A. Dujella, Uvod u teoriju brojeva, skripta, Matematički odjel, Sveučilište u Zagrebu, 2009.

[2] A. Dujella, Teorija brojeva u kriptografiji, skripta, Matematički odjel, Sveučilište u Zagrebu, 2003/2004

[3] J. Hoffstein, J. Pipher, J. H. Silverman, An introduction to mathematical cryptography, Springer, New York, 2008.

[4] I. Matić, Uvod u teoriju brojeva, skripta, Odjel za matematiku, Sveučilište J.J. Strossmayera, Osijek, 2013.